SARA BETH CRAIG (BAR NO. 301290)
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
555 Montgomery Street, Ste. 820
San Francisco, CA 94111
Telephone: 415-766-3544
Facsimile: 415-840-9435
Email: scraig@peifferwolf.com

Counsel For Plaintiffs

[Additional Counsel On Signature Page]

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

TREVOR LAKES, and ALEX RAJJOUB on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. UBISOFT, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Trevor Lakes and Alex Rajjoub ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this class action complaint against Ubisoft, Inc. (the "Ubisoft" or "Defendant"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who: (i) visited https://www.ubisoft.com/ (the "Website"), operated by Defendant; and, either (a) purchased a video game on the Website (the "Purchasers"), or (b) subscribed to the Website's Ubisoft+ service,

which allowed users to gain access to video games on the Website (the "Subscribers") (collectively, the "PII Users").

2. The Website provides users with the ability to search for, purchase, and download video games produced or published by Defendant.

3. Similarly, the Website allows users to pay a recurring fee to gain access to an "Ubisoft+" subscription, which gives Subscribers access to games so long as the subscription is maintained, with the highest tier of Ubisoft+ giving users access to more than 100 video games, including premium editions of video games, exclusive content, and monthly in-game rewards.[1]

4. Defendant does not disclose on the Website that PII Users' personally identifying information ("PII") would be captured by the Meta Platforms, Inc. ("Meta" or "Facebook") tracking Pixel (the "Pixel") utilized by Defendant, and then transferred to Meta thereby exposing the subscribers' PII to any person of ordinary technical skill who received that data.

5. Data sharing policies for a service or subscription is an important factor for individuals deciding whether to provide personal information to that service.

6. Congress has recognized the immediate and irreversible harm caused by associating a person's personally identifiable information in conjunction with a list of specific audio-visual materials they have requested or consumed.

7. The Video Privacy Protection Act ("VPPA") prohibits video tape service providers,[2] such as Defendant, from sharing PII. Under the VPPA, PII is information that can specifically tie the identity of an individual to the individual's requested pre-recorded audio video material, either through the title, description, or summary of the video content.[3]

8. Congress made clear that harm to an individual impacted by a VPPA violation occurs the moment, and each time, a consumer's information is shared.

9. Defendant purposefully implemented and utilized the Pixel, which tracks user activity on the Website and discloses that information to Facebook to gather valuable marketing

---

[1] *Ubisoft Store*, UBISOFT, https://store.ubisoft.com/us/ubisoftplus?lang=en_US (last visited September 16, 2024).
[2] 18 U.S.C. § 2710(a)(4).
[3] 18 U.S.C. § 2710(b)(2)(D)(II).

data. The Pixel cannot be placed on a Website without steps taken directly by Defendant or on behalf of Defendant (e.g., by a website manager). The Pixel cannot be placed on the Website by Facebook without the knowledge and cooperation of Defendant.

10. Defendant does not seek, and have not obtained, consent from PII Users to utilize the Pixel to track, share, and exchange their PII with Facebook.

11. Defendant knew that their Pixel resulted in users' PII and search terms being shared (resulting in VPPA and Wiretap Act violations), and that they failed to obtain users' consent to allow their Pixel to operate in a way that shares users' protected information with Facebook.

12. PII Users of the Website have been harmed as a result of Defendant's violations of the VPPA and Wiretap Act. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Pixel from the Website, or (ii) add, and obtain, the appropriate consent from PII Users; or otherwise anonymize video game titles in URLs, parameters, and metadata and/or hash PII Users' Facebook user IDs ("FIDs") in the Pixel transmissions.

13. Federal legislatures addressed citizens privacy expectations when communicating with parties over wired communications.

14. Congress passed the Wiretap Act, which prohibits the unauthorized interception of electronic communications.

15. Defendant purposefully implemented and utilized the Pixel to intercept and read the search terms and disclose the location and content of webpages visited by PII Users.

16. Finally, Plaintiffs had their privacy interests violated.

17. PII Users of the Website, such as Plaintiffs, have an interest in maintaining control over their private and sensitive information, such as their PII and search terms, as well as an interest in preventing their misuse.

18. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of PII Users of the Website for violations of the VPPA and the Wiretap Act.

19. Defendant violated the VPPA the moment, and each time, Plaintiffs and Class Members requested, obtained, or watched a video on the Website and had their PII shared.

20. Defendant violated the Wiretap Act the moment, and each time, Plaintiffs and Class Members submitted search terms leading to video content on the Website.

PARTIES

21. Plaintiff Trevor Lakes is a citizen of California who resides in North Hills, California. Plaintiff Lakes visited the Website while logged into his Facebook account, and subscribed to the Ubisoft+ service on September 7, 2024. Thereafter, Plaintiff Lakes used the Website on his Chrome browser, while logged into his Facebook account, to download at least one video game containing cinematics or cut scenes.[4] The video games downloaded by Plaintiff Lakes include cut scenes and cinematics. Plaintiff Lakes' Facebook profile includes his name, location, occupation, photos, relationship status, friend list, and posts.

22. Plaintiff Alex Rajjoub is a citizen of West Virginia who resides in Morgantown, West Virginia. Plaintiff Rajjoub visited the Website while logged into his Facebook account, to purchase at least one video game containing cut scenes.[5] Thereafter, Plaintiff Rajjoub visited the Website on his Chrome browser, while logged into his Facebook account, to download at least one video game, which contained cut scenes and cinematics. Plaintiff Rajjoub's Facebook profile includes his first name, location, occupation, photos, relationship status, friend list, and posts.

23. Defendant Ubisoft, Inc. is headquartered in San Francisco, CA and serves as a business office and video game development studio, with nearly 500 employees in marketing, sales, business development, communications, finance, licensing, and game development.

JURISDICTION AND VENUE

24. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the aggregate amount in controversy exceeds

[4] Plaintiff Lakes requested and downloaded Star Wars Outlaws, Immortals Fenyx Rising, and Rayman Legends, among other games.

[5] Plaintiff Rajjoub purchased Tom Clancy's Rainbow 6 Siege, Assassin's Creed, and Far Cry video games.

$5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from at least one Defendant.

25. This Court has personal jurisdiction over Defendant because Defendant Ubisoft's principal place of business is in California, and Defendant derive revenue in the State of California, including the Defendant's revenue generation from its management and operational control over the Website, as well as the revenue sharing, advertising sales, etc. that the Defendant derive from the Website.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and Defendant conducts substantial business operations in this District, including managing the Website, delivery of video games, and Defendant's U.S.-based marketing.

27. **Divisional Assignment:** Assignment to this Division is proper because Defendant's principal place of business is in San Francisco, California, and a substantial part of the events or omissions giving rise to the claim occurred there.

FACTUAL BACKGROUND

I. The VPPA

28. The VPPA was first conceived of because of an incident stemming from President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a reporter requested Judge Bork's movie rental history from the rental establishment. The employee disclosed to Judge Bork's movie rental history to the Washington City Paper which then published that history. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator Patrick Leahy, who introduced the Act, explained:

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong.

S. Rep. 100-599, at 5-6 (internal ellipses and brackets omitted).

29. Senators were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audio-visual materials. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

30. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

31. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy stated that "[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[6]

32. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

33. The VPPA defines personally identifiable information ("PII") as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3).

34. A video tape service provider ("VTSP") is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video

[6] See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited on September 16, 2024).

cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4). A consumer is "any renter, purchaser, or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1).

35. The VPPA also prohibits the disclosure of PII which identifies the title or description of the audio visual material for marketing goods and services. 18 U.S.C. § 2710(b)(2)(D)(ii).

36. VTSPs may obtain consent from consumers to disclose information where that consent: 1) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer (18 U.S.C. § 2710(b)(2)(B)(i)); 2) at the election of the consumer in advance of up to 2 years or when the disclosure is sought (18 U.S.C. § 2710(b)(2)(B)(ii)); and; 3) if the VTSP provided the consumer with a clear and conspicuous opportunity to withdraw consent on a case-by-case basis or withdraw from ongoing disclosures at the consumer's election (18 U.S.C. § 2710(b)(2)(B)(iii)).

37. Under the statute, for each violation of the statute, a court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief, and attorney's fees.

38. Defendant here are video service providers in that they sold or provided access to pre-recorded audio-visual materials to PII Users, including Plaintiffs and Class Members, on their Website.

39. The relationship between Plaintiffs and Defendant is precisely the type of relationship contemplated by the VPPA.

40. In this case, Defendant knowingly and systematically disclosed Plaintiffs' personally identifiable information to Meta, without obtaining their consent, by purposely placing the Pixel on the Website with the knowledge it would collect user information.

II. The VPPA and Video Games

41. The VPPA covers "prerecorded video cassette tapes or similar audio visual materials," see 18 U.S.C. § 2710(a)(4), and Congress intended that to include broad category of audio visual materials, including "laser discs, open-reel movies, or CDI technology" (see S. Rep.

100-599), digitally streamed "video clips[,]" and video game cutscenes. *See Aldana v. GameStop, Inc.*, 2024 U.S. Dist. LEXIS 29496, at *17-18, 19 (S.D.N.Y. Feb. 21, 2024).

42. Video games have contained "cut scenes"[7] since the 1980s, and are designed to "keep players immersed in the game world by allowing them to follow a clear narrative."[8]

43. "Narrative storytelling has become more and more common in video games . . . [and] [u]sing cinematic techniques and principles has helped game developers enhance gameplay experience for these kinds of games."[9]

44. As early as 1981, laser discs "permit[ted] the viewer to not only manipulate the programming, but to interact with the material – play games, take quizzes, adjust pacing and repeat sections as desired."[10] VHS tapes could also contain interactive content, like the television series "Captain Power and the Soldiers of the Future," which used "video game technology" to create an interactive experience, emitting "a signal, encoded in the television film, that both activates and responds to light rays emitted by the toy – a jet aircraft with a pistol grip – when the user pulls the trigger."[11]

45. By the mid-1980s, Philips and Sony announced the development of a new video game medium based on the CD and CD-ROM technology.[12] This new format, called Compact-Disc Interactive, or CD-I, was developed to store larger volumes of combined audio, video, and computer graphics on a compact disc.[13]

---

[7] Cut scenes, also called cinematics, full motion videos, or interactive events, exist in several formats, including live action video, pre-rendered cut scenes, and real time cut scenes. Each method makes use of pre-scripted events, and audio and video materials stored within a game's files. *See* David 'Ryatta' Wyatt, *The Art of Cutscenes*, INMOTION GAMING, http://www.inmotiongaming.com/the-art-of-cutscenes/ (last visited September 16, 2024).

[8] *Game Development Meets Filmmaking: Cinematography in Video Games*, ACAD. OF ART UNIV. BLOG (Feb. 21 2020), https://blog.academyart.edu/game-development-meets-filmmaking-cinematography-in-video-games/ (last visited September 17, 2024).

[9] *Id.*

[10] Myron Berger, *High-Tech Equipment Comes of Age*, N.Y. TIMES (Oct. 4, 1987).

[11] Sandra Salmans, *The Interactive World of Toys and Television*, N.Y. TIMES (Oct. 4, 1987).

[12] *See* Scott A. Stewart, *Videodiscs in Healthcare: A Guide to the Industry*, THE MEDICALDISC REPORTER (1990), *archived at* https://tinyurl.com/44ypcaht (last visited September 17, 2024).

[13] *See* ENCYCLOPEDIA OF LIBRARY AND INFORMATION SCIENCE 98 (1992), *archived at* https://tinyurl.com/mt2vutat (last visited September 17, 2024).

46. By 1991, Philips introduced the Philips CDI 910, which "play[ed] cinema-quality computer games, educational programs, movies, and other multimedia products that combine video, audio and text features in an interactive rather than a play-only mode."[14] The Philips CDI 910 played games like "Voyeur," for example, which was "a kind of high-tech version of Clue[,]"allowing users to "make decisions for characters and even change the outcome of the mystery."[15]

47. Sony unveiled its own console, the "Play Station," which used a CD-ROM drive to "play videogames as well as other forms of interactive entertainment, as was considered important at the time."[16]

48. These technologies blurred the line between video games and movies, as "more and more movies look and sound like video games, and . . . more and more video games look and sound like movies . . . ."[17]

49. The advancement of these technology has also opened the door for actors to take greater part in a video game's narrative, with game developers using performance capture technology to record and translate actors' movements and facial expressions,[18] in addition to traditional acting performances.[19]

---

[14] Patrick Oster, *Philips's Multimedia Makeover; Dutch Electronics Firm Escapes Crisis, but Can It Compete Globally?*, WASH. PO. (Oct. 26, 1994), *archived at* https://tinyurl.com/4xwnausj (last visited September 17, 2024).

[15] David Elrich, *Interactive Video: Armchair Activities*, N.Y. TIMES (Dec. 9, 1993), *archived at* https://nyti.ms/3Wp2wkZ (last visited September 17, 2024).

[16] IGN Staff, *History of the PlayStation: The greatest story ever told*, IGN (June 21, 2012), *available at https://tinyurl.com/25245e9t* (last visited September 17, 2024).

[17] Vincent Canby, *Are Video Games About to Zap the Action Movie?*, N.Y. TIMES (May 15, 1983), *archived at* https://tinyurl.com/5fv5s6v3 (last visited September 17, 2024).

[18] *See* Anton Söderhäll, *Tracing the past, present, and future of game cinematics*, Games Industry (Jan. 25, 2022), https://www.gamesindustry.biz/tracing-the-past-present-and-future-of-game-cinematics (last visited September 17, 2024).

[19] *See* Adam Sutton, *Videogame Voice Acting: So Bad, It's Good*, IGN (Jun. 14, 2012 1:29 PM), https://www.ign.com/articles/2011/03/04/videogame-voice-acting-so-bad-its-good (last visited September 17, 2024); Jesse Schedeen, *Cyberpunk 2077, Keanu Reeves and 12 Other Movie Stars Who Made the Jump to Video* Games, IGN (Jan. 14, 2020 12:25 PM), https://www.ign.com/articles/2019/06/11/cyberpunk-2077-keanu-reeves-and-12-other-movie-stars-who-made-the-jump-to-video-games (last visited September 17, 2024).

50. In the episode "How Cinematic Cutscenes in Video Games are Made" of "A Game Development Podcast," which is produced by Massive Entertainment, an Ubisoft Game development studio, Cinematic Animator Soo Kang notes the basic purpose of a cinematic animator is "responsible for making the visual story telling of the game exciting, inspirational, fun, engaging, making sure that what you're seeing, on screen, the story telling, helps you progress with your gameplay as well . . . but just in general just fun to watch while you're sitting and taking a little break from gameplay . . . ."[20]

51. Soo Kang highlights the similarities between modern game cinematic production and film animation production: "[I]t just happened that I got my job in gaming industry first, but it wasn't too far off from what I learned about film animation because it was cinematic animation, . . . as opposed to game play animation for example . . . so they were not too far off."[21]

52. Soo Kang went on to note that the difference between film and cinematic animation was not big because she was "applying the same learnings of the cinematic scene in the film, just in the game . . . maybe the transition is different . . . but, like, it wasn't, it didn't feel like I was starting from or reset from zero[.]"[22]

53. These advancements in game production were enabled by the technical advancement in mediums used to store video games. Today, video games are typically

[20] Massive Entertainment – A Ubisoft Studio, *How Cinematic Cutscenes in Video Games are Made | A Game Development Podcast*, YOUTUBE (Nov. 23, 2022), https://www.youtube.com/watch?v=WVQgeCZLjek (starting at 1:34) (last visited September 17, 2024).

[21] *Id.* (starting at 6:22).

[22] *Id.* (starting at ; *Id.* (starting at 6:55).

manufactured using 100GB Blu-ray discs, the same audio-visual material used for movies.[23] Video games are also made available for download, with similar file sizes.[24]

III. How Websites Function

54. Websites are hosted on servers, in the sense that their files are stored on and accessed from servers, however, websites are, in part, "run" on a user's internet browser, as the browser loads and processes the website's code to display the webpage.

55. Websites are a collection of webpages. A webpage is essentially a document containing text written in HyperText Markup Language (HTML) code.[25]

56. Each webpage has a unique address, and two webpages cannot be stored at the same address.[26]

57. When a user navigates to a webpage (by entering a URL address directly or clicking a hyperlink containing the address), that user's browser contacts the DNS (Domain Name System) server, which translates the web address of that website into a unique IP (Internet Protocol) address.[27]

---

[23] Chaim Gartenberg, *Sony confirms PlayStation 5 name, holiday 2020 release data*, THE VERGE (Oct. 8, 2019) ("[T]he PS5 will use standard 100GB Blu-ray discs—Sony had previously confirmed that the console will offer a disc drive—but all games will have to be installed in the internal SSD this time around."), *available at* https://tinyurl.com/3z9spd9x (last visited September 17, 2024); *see also* Samuel Tolbert, *Can you use physical discs on PS5?*, ANDROID CENTRAL (Dec. 1, 2020) ("Cerny also confirmed that PS5 games are going to shop on 100GB Blu-ray discs."), *available at https://tinyurl.com/uchzpvt9* (last visited September 17, 2024).

[24] As an example, Avatar: Frontiers of Pandora, a game available for sale on the Website, requires a minimum of 90GBs of storage. *See Avatar: Frontiers of Pandora – Standard Edition*, UBISOFT, https://store.ubisoft.com/us/avatar--frontiers-of-pandora/60c30ca40d253c1914049e93.html?lang=en_US (last visited September 17, 2024).

[25] *What is the difference between webpage, website, web server, and search engine?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines (last visited September 17, 2024).

[26] *Id.*

[27] *How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited September 17, 2024).

58. An IP address is "a unique address that identifies a device on the internet or a local network."[28] Essentially, an IP address is:

> the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

Id.

59. When a user's browser navigates to a webpage, it sends an HTTP request to the server identified by the webpage's IP address. This request is for the specific resource located at the URL. If the server fulfills this request, it issues an HTTP response, which includes the status of the request and, typically, the requested content. This content is then transmitted in small chunks, known as data packets, and reassembled into the complete webpage upon arrival by the user's browser.[29]

60. This Request URL includes a domain name and path, which identify the specific content being accessed on a website and its location within the website's structure.

61. The Request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters. Parameters direct a web server to provide additional context-sensitive services,[30] as depicted below:

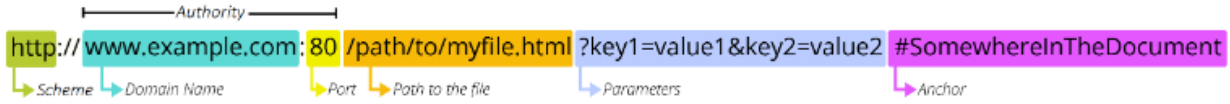

Figure 1 - Mozilla's diagram of a URL, including parameters[31]

---

[28] *What is an IP Address – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address (last visited September 17, 2024).

[29] *Id.*

[30] To see examples of how Ubisoft used parameters to provide additional information here, *see, infra,* Section V.

[31] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited September 17, 2024).

62. The user's browser then assembles the small chunks back into HTML, which is then processed by the user's browser and "rendered" into a visual display according to the instructions of the HTML code.[32] This is the visible, and usually interactable, website that most people think of.

63. To provide more complex website functionalities, website developers will include more complex commands written in other computer programming languages such as JavaScript snippets within the HTML documents.[33]

64. Such complex tasks include making video games downloadable by users who purchased video games or otherwise have an Ubisoft+ subscription, or code used to monitor and report user activity.

IV. The Facebook Tracking Pixel

65. Boasting 2.9 billion monthly active users, Facebook is the largest social networking site on the planet.[34] Facebook is a "real identity platform,"[35] meaning users are allowed only one account and must share "the name they go by in everyday life."[36] To meet that goal, Facebook requires users, when creating an account, to provide their first and last name, along with their birthday and gender.[37]

66. Facebook monetizes users by selling advertisers access to their Facebook feeds.[38]

---

[32] *Id.*

[33] *See JavaScript Basics*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/JavaScript_basics (last visited September 17, 2024).

[34] Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, Yahoo (July 28, 2021), https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html (last visited September 17, 2024).

[35] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[36] *Community Standards, Part IV Integrity and Authenticity*, FACEBOOK, https://www.facebook.com/communitystandards/integrity_authenticity (last visited September 17, 2024).

[37] *Sign Up*, FACEBOOK, https://www.facebook.com/ (last visited September 17, 2024).

[38] Mike Isaac, *Facebook's profit surges 101 percent on strong ad sales.*, N.Y. TIMES (July 28, 2021), https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html (last visited September 17, 2024).

67. Facebook's advertising capabilities are valuable because of its ability to effectively target users with meaningful or relevant advertising.[39] Facebook can target users so effectively because it monitors and analyzes user activity both on and off its site.[40] This allows Facebook to infer details about users beyond what users explicitly disclose, like their "interests," "behavior," and "connections."[41] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers can sort through using highly specific filters and parameters to make sure their targeted advertisements are aimed at users likely to positively respond.[42]

68. Advertisers can build "Custom Audiences,"[43] which enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[44] Meta's Custom Audience feature enables the direct targeting of existing customers and to build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[45] Unlike Core Audiences, Custom Audiences require an advertiser to supply users' data to Facebook. Advertisers can do so through two

[39] *Why Advertise on Facebook*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited September 17, 2024).

[40] *About Facebook Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited September 17, 2024).

[41] *Ad Targeting: Help your ads find the people who will love your business,* FACEBOOK, https://www.facebook.com/business/ads/ad-targeting (last visited September 17, 2024).

[42] *Easier, More Effective Ways to Reach the Right People on Facebook*, FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited September 17, 2024).

[43] *About Custom Audiences*, FACEBOOK, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited September 17, 2024).

[44] *About Events Custom Audience*, FACEBOOK, https://www.facebook.com/business/help/366151833804507?id=300360584271273 (last visited September 17, 2024).

[45] *About Lookalike Audiences*, FACEBOOK, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited September 17, 2024).

mechanisms: by manually uploading contact information for customers in the form of "lists," or by utilizing Facebook's "Business Tools," which collect and transmit the data automatically.[46]

69. Here, Ubisoft employs both methods of supplying user information to Meta.

70. Meta's "Business Tools" allow web developers to monitor user interactions on their websites, which can then be shared with Meta. For example, Meta offers a tracking Pixel (the "Pixel") and the Conversions API. Where "the Pixel lets you share web events from a web browser[,] . . . the Conversions API lets you share web events directly from your server."[47]

71. The Pixel is a piece of code that advertisers, like Defendant, can integrate into their website. Once activated, the Pixel "tracks the people and type of actions they take."[48] When the Pixel captures an action, it sends a record of the action to Facebook. After receiving the Pixel transmission sent by an advertiser, Facebook processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences.

72. After processing the data, Meta also makes much of the data available to the advertisers through the "Event Manager" tool.[49]

73. However, to make use of the Pixel, Defendant must first agree to the Meta Business Tools Terms.

74. The Meta Business Tools Terms directly inform Pixel users how the Pixel operates.

75. Meta explicitly informs Pixel users that using the Pixel will result in Facebook receiving users' information ". . . that personally identifies [them] . . . " ("Contact Information") and information ". . . about [users] and the actions they take on your websites . . ." ("Event

---

[46] *Create a Customer List Custom Audience*, FACEBOOK, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited September 17, 2024); *Create a Website Custom Audience*, FACEBOOK, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited September 17, 2024).

[47] *Business Help Center: About deduplication for Meta Pixel and Conversions API events*, FACEBOOK, https://www.facebook.com/business/help/823677331451951?id=1205376682832142 (last visited September 17, 2024).

[48] *Retargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting (last visited September 17, 2024).

[49] *About Meta Events Manager*, FACEBOOK, https://www.facebook.com/business/help/898185560232180?id=1205376682832142 (last visited September 17, 2024).

Data").[50] The terms also warn website developers that Facebook will "process the Contact Information solely to match the Contact Information against" FIDs, "as well as to combine those [FIDs] with corresponding Event Data."[51]

76. Meta also requires Pixel users to "represent and warrant that [they] . . . have all the necessary rights and permissions and a lawful basis (in compliance with all applicable laws, regulations and industry guidelines) for the disclosure and use of Business Tool Data."[52]

77. Additionally, Meta requires Pixel users to "represent and warrant that [they] will not share Business Tool Data with [Meta] that . . . includes . . . categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)." [53]

78. In short, Meta explicitly explains that the Pixel combines users' identifying information with their activity on websites to build marketing profiles and, as a result, that websites should not share sensitive information using the Pixel.

79. Despite Meta's warnings, advertisers ultimately have control over what actions—or, as Facebook calls it, "events"—the Facebook Tracking Pixel will be active on websites. These events, in turn, determine what data is collected, including the website's query string parameters, metadata, and what pages a visitor views.[54]

80. Advertisers can also configure the Facebook Tracking Pixel to track events other than Meta's menu of "standard events," which contain events that can track what content a visitor

---

[50] *Meta Business Tools Terms*, *Section 1(a)(i)-(ii)*, FACEBOOK, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfY4CZdRHnQNL2-VtXBCcMUcg-6J-5jU8AL4hOLViKhAWi-SbNmA4QuXlc6yyk877eY&_rdr (last visited September 17, 2024).

[51] *Id.* at Section 2(a)(i)(1).

[52] *Id.* at Section 1(e).

[53] *Id.* at Section 1(h).

[54] *See Facebook Pixel, Accurate Event Tracking, Advanced*, FACEBOOK, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited September 17, 2024); *see also Best Practices for Facebook Pixel Setup*, FACEBOOK, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited September 17, 2024).

views or purchases.[55] An advertiser can also create their own "custom events," allowing them to track designated user activity and data through events programmed specifically for that purpose on advertiser's website.[56]

81. Advertisers also control how the Facebook Tracking Pixel identifies visitors. The Facebook Tracking Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific Data."[57]

82. HTTP Headers include "IP addresses, information about the web browser, page location, document, referrer and data potentially identifying persons using the website."[58]

83. Pixel-specific Data includes "the Pixel ID and cookie[s],"[59] which can also identify persons using the website.

84. Once a Pixel activates, it copies relevant information from the communication between the user and Website, such as URLs, user activity, search terms, metadata, query string parameters, and cookies, bundle that information together, and transmits that copied bundle to Meta through a "GET" or "POST" HTTP request.

V. Ubisoft And The Facebook Pixel

85. The Website offers users multiple ways to request and obtain video games: 1) direct purchases through the Website; and 2) subscriptions to Ubisoft+, ranging from $6.67 a month to $17.99 a month.[60]

86. While both require making an account with Ubisoft, direct purchases allow the user to access purchased video games with or without a subscription.

---

[55] *Specifications for Facebook Pixel Standard Events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited September 17, 2024).

[56] *About Standard and Custom Website Events*, FACEBOOK, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited September 17, 2024).

[57] *Facebook Pixel*, FACEBOOK, https://developers.facebook.com/docs/facebook-pixel/ (last visited September 17, 2024).

[58] *Id.*

[59] *Id.*

[60] *Ubisoft+*, UBISOFT, https://store.ubisoft.com/us/ubisoftplus?lang=en_US (last visited September 17, 2024).

87. Ubisoft+ gives users access to games so long as the subscription is maintained, with the highest tier of Ubisoft+ giving users access to more than 100 video games, including premium editions of video games, exclusive content, and monthly in-game rewards.[61]

88. Ubisoft added the Pixel to its Website, which it uses to track customers throughout their use of the Website and through the purchase process.

89. When a user searches for a video game, for example, Ubisoft discloses data via the PageView event.

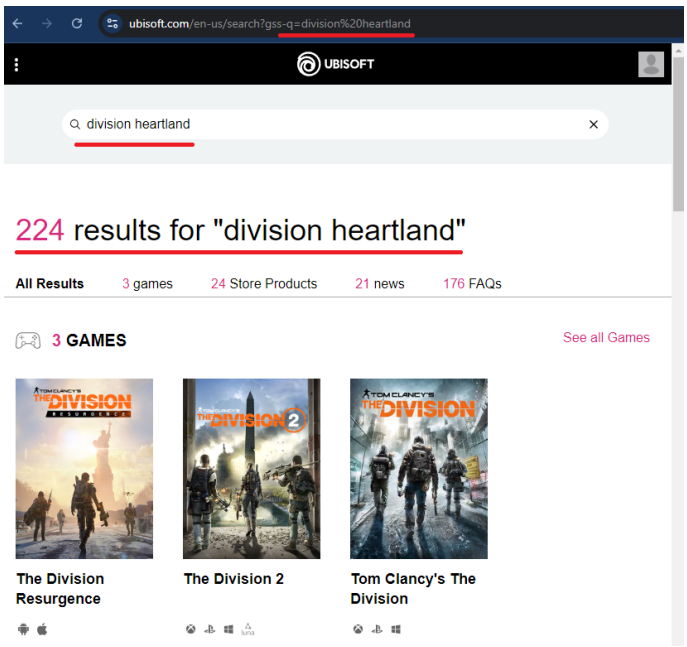

Figure 22 - Sample search on the Website using search terms "division heartland"

90. PageView data discloses what video games a user has searched.

[61] *Id.*

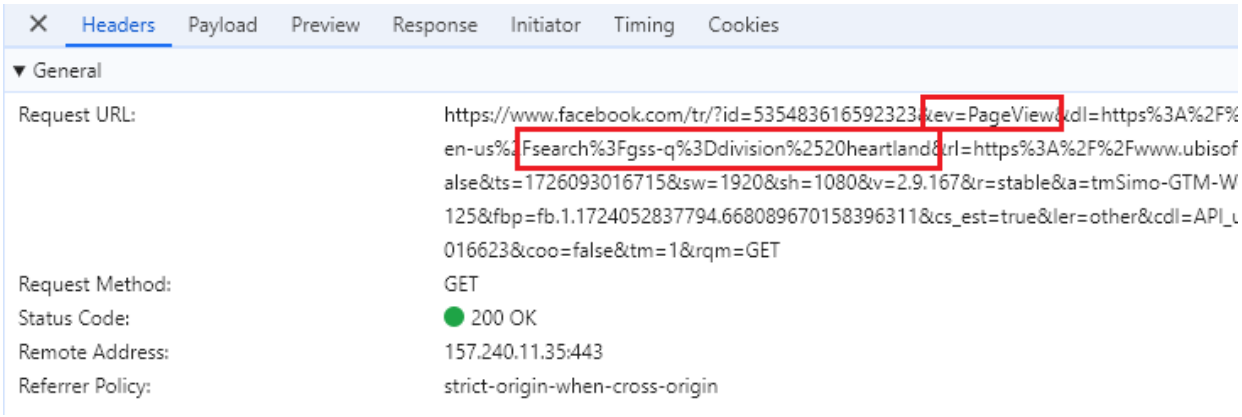

Figure 33 - Pixel transmission containing search terms entered by users

91. When a consumer clicks on the searched game, another PageView event is triggered, transmitting the video game's title.

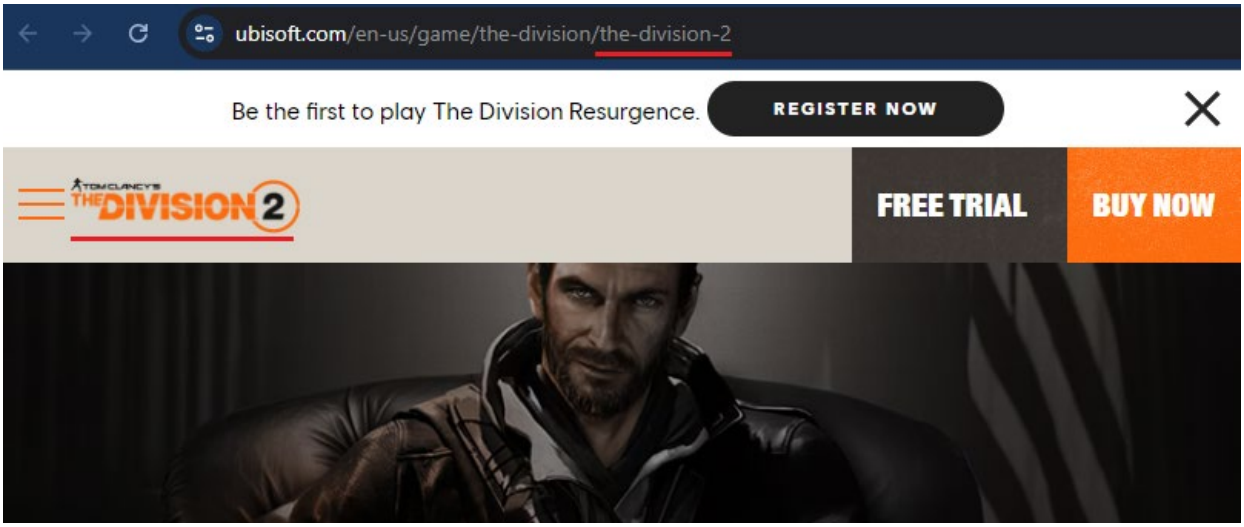

Figure 4 - Webpage resulting from click-on search result, including game title

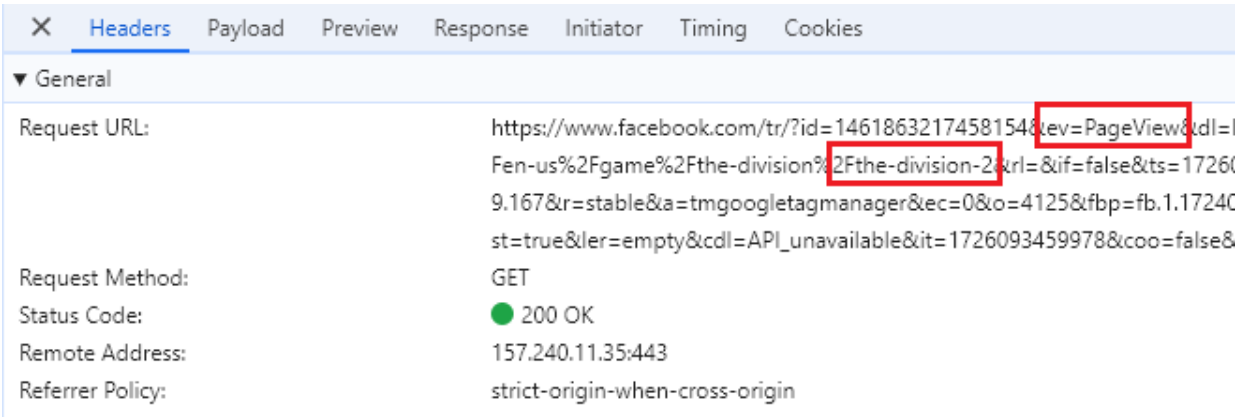

Figure 5 - Pixel transmission caused by clicking on search result, including video game title

92. Ubisoft then uses the "AddToCart" events to trigger when users click the button to add video games to their digital shopping carts, as well as the PageView and "ViewContent" events when the user is forced to load the checkout webpage after clicking "Buy", disclosing the title of the video game being purchased or downloaded.

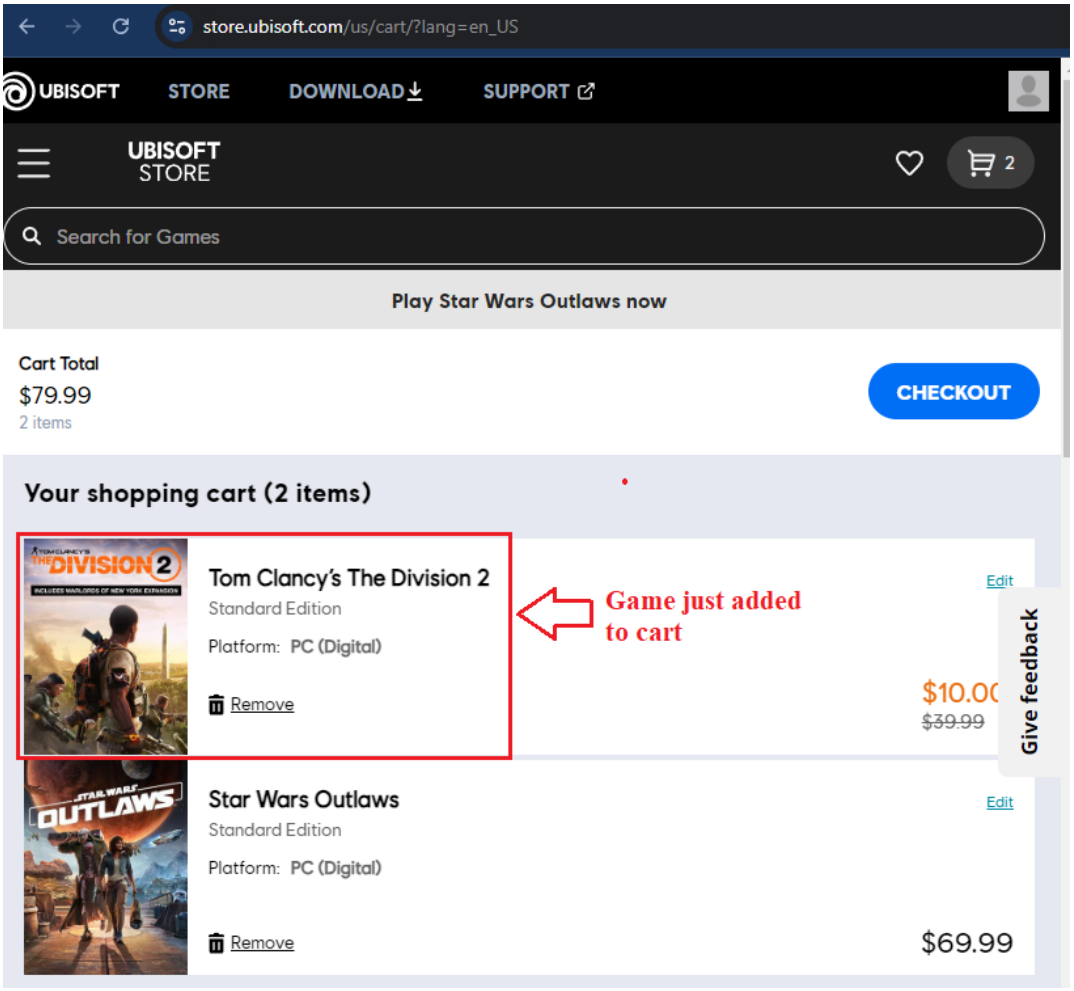

Figure 6 - Resulting webpage from clicking on button to obtain video game

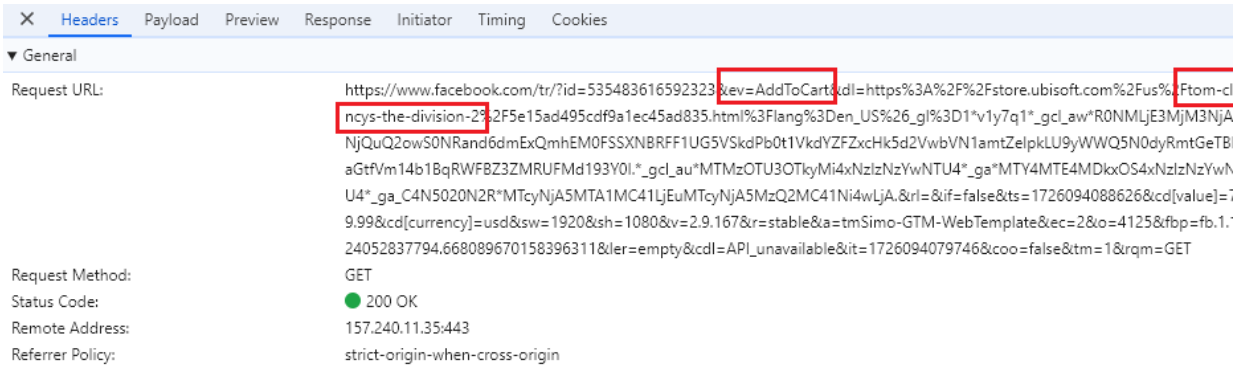

Figure 7 - Pixel transmission resulting from clicking button to add game to cart, including game title

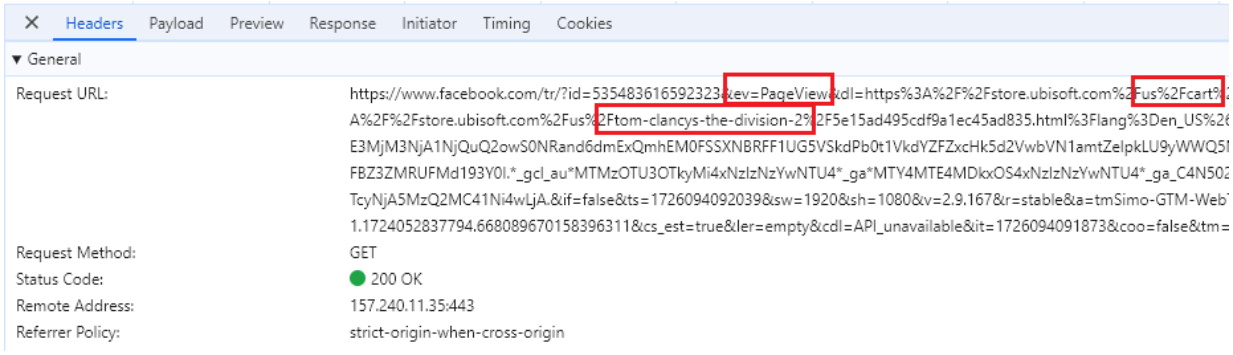

Figure 8 - Pixel transmission resulting from loading cart webpage, including game title

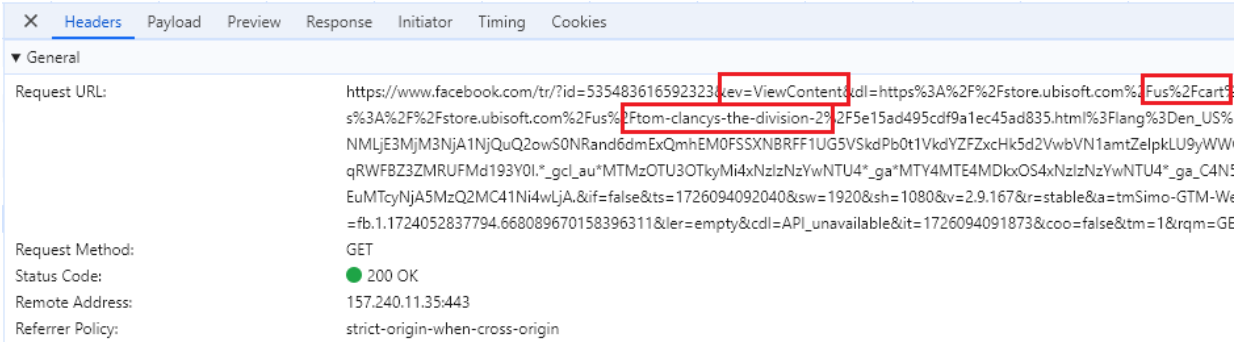

Figure 9 - Pixel transmission resulting from loading cart webpage, including game title

93. Ubisoft monitors when users navigate to the checking out webpage on the Website via the PageView and View Content events.

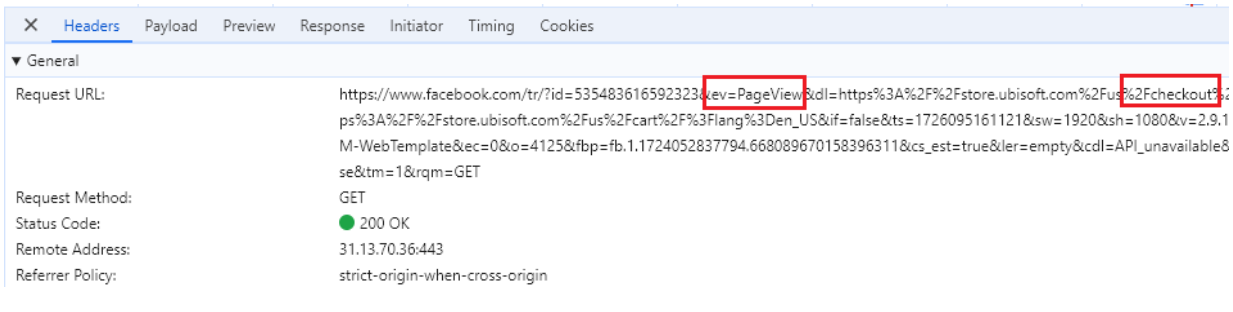

Figure 10 - Pixel transmission resulting from loading checkout webpage

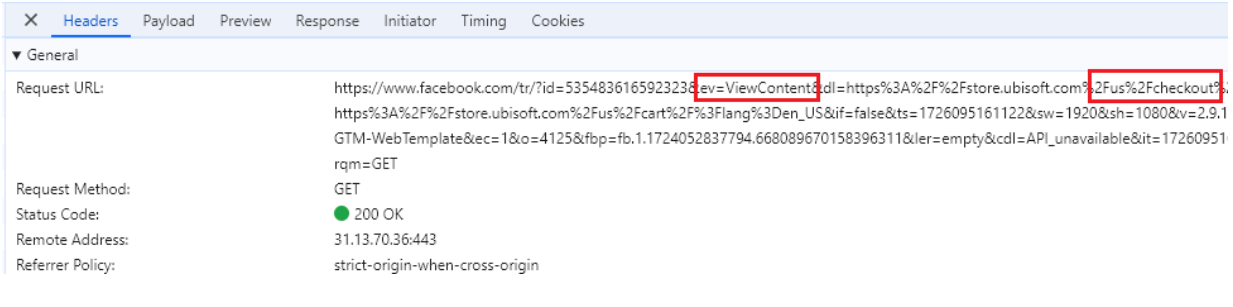

Figure 11 - Pixel transmission resulting from loading checkout webpage

94. To checkout, a user must click the purchase button.

95. Ubisoft uses the ViewContent, Purchase, and PageView events to monitor when a user completes a purchase.

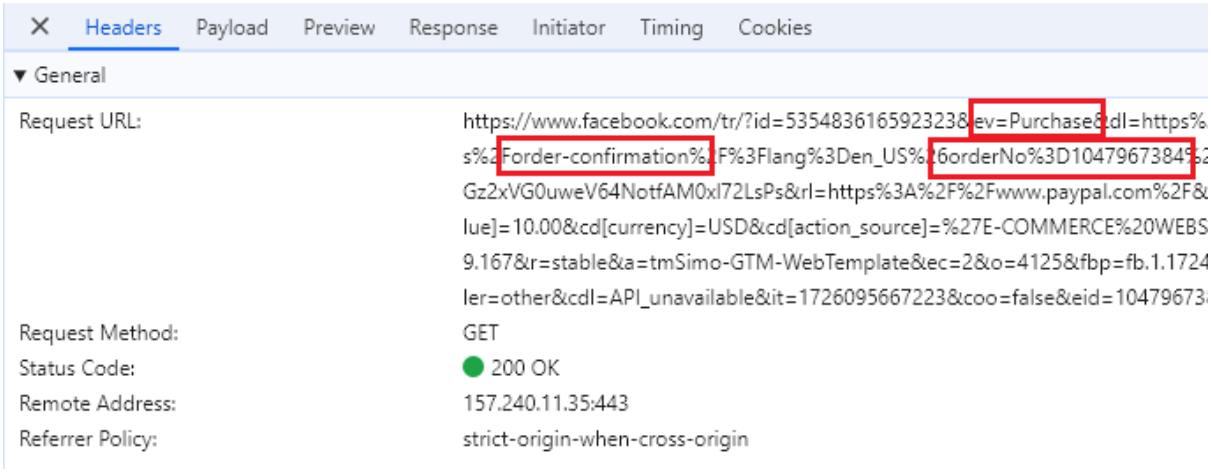

Figure 12 - Pixel transmission resulting from completing purchase process

96. The event data disclosed by Ubisoft permits an ordinary person to identify a purchased video game.

97. When a consumer purchases a video game while logged into Facebook, Ubisoft compels a visitor's browser to transmit to Facebook the c_user cookie, which contains that visitor's unencrypted Facebook ID (the "FID"). When purchasing the above game, for example, Defendant compelled the browser to send eight cookies, seven of which are visible here:

Figure 13 - Cookies attached to Pixel transmission

98. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[62] The datr cookies also identifies a browser.[63] Facebook, at a minimum, uses the fr and _fbp cookies to identify users.

99. Without a corresponding Facebook ID, the fr cookie contains, at least, an abbreviated and encrypted value that identifies the browser. Facebook uses this cookie for targeted advertising.

100. The fr cookie will expire after 90 days unless the visitor's browser logs back into Facebook.[64] If that happens, the time resets, and another 90 days begins to accrue.[65]

101. Facebook, at a minimum, uses the fr and c_user cookies to link to Facebook IDs and corresponding Facebook profiles.

102. An FID is personally identifiable information. It contains a series of numbers used to identify a specific profile, as depicted below:

Figure 14 - Sample c_user ID number of test account created by Plaintiffs' counsel to investigate the Pixel, captured by a Pixel event

103. A FID can be used by anyone to easily identify a Facebook user by simply appending the FID to www.facebook.com (e.g., www.facebook.com/[UID_here]).

---

[62] *Report of Re-Audit*, DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD (Sept. 21, 2012) http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited September 17, 2024).
[63] *Cookies & other storage technologies*, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited September 17, 2024).
[64] *See* COOKIES & OTHER STORAGE TECHNOLOGIES, FACEBOOK, https://www.facebook.com/policy/cookies/ (last visited September 17, 2024).
[65] Confirmable through developer tools.

104. Using the FID from Figure 14, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the FID, as depicted below:

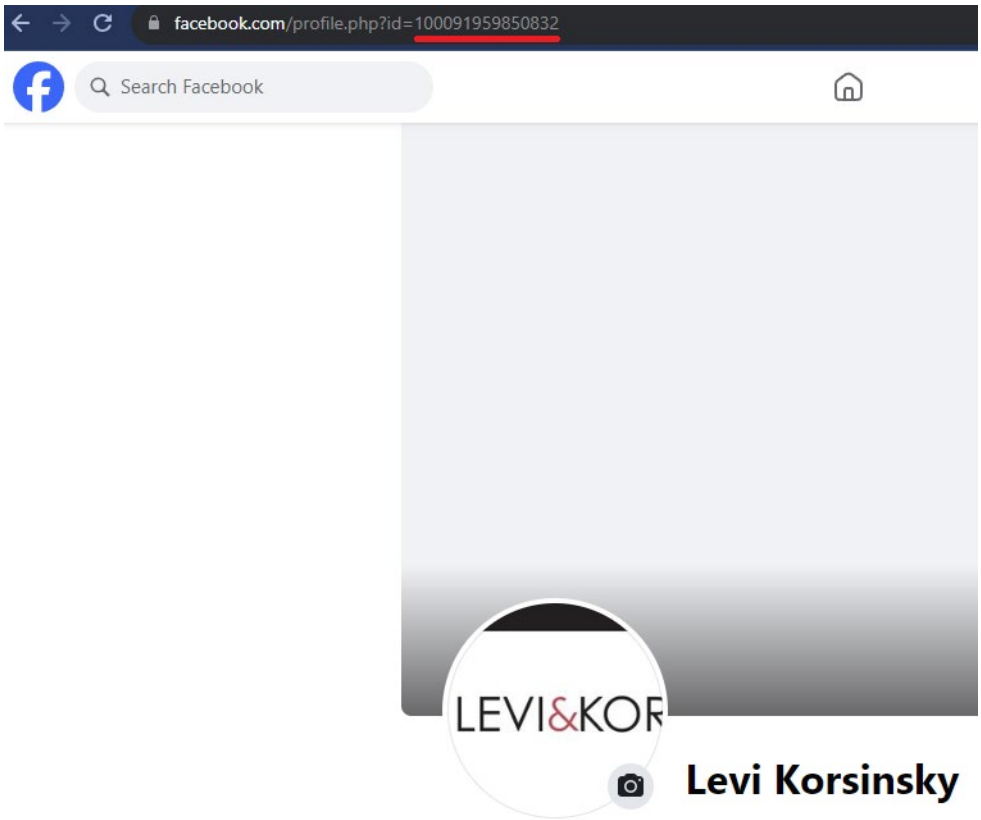

Figure 15 - Appending FID of a user to "facebook.com/" results in the user being redirected to the user's profile

105. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language and country – are "always public."[66] No privacy setting on a Facebook account would allow Plaintiffs, or any users, to hide this basic information.

106. By compelling a visitor's browser to disclose the c_user cookie alongside event data for video games, Ubisoft knowingly discloses information sufficiently permitting an ordinary person to identify what video games a specific individual has purchased.

[66] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited September 17, 2024).

107. By compelling a visitor's browser to disclose the fr cookies alongside event data for video games, Ubisoft knowingly discloses information sufficiently permitting an ordinary person to identify what video games a specific individual has purchased.

108. By compelling a visitor's browser to disclose the fr cookie and other browser identifiers alongside event data for video games, Ubisoft knowingly discloses information sufficiently permitting an ordinary person to identify what video games a specific individual has purchased.

109. Defendant also uploads customer lists to Meta that contain PII Users' email addresses and purchase information, including what video games they purchased or downloaded. Defendant uploads these lists to Meta so that Meta can match PII Users to their Facebook profiles.

110. Meta admits that "[advertisers] provide us with information about [their] existing customers and we match this information with Facebook profiles."[67] The customer lists must contain "'identifier[s]' (such as email, phone number, address)"[68] so that Meta can match the lists to "Facebook profiles" and "[advertisers] can advertise to [their] customers on Facebook, Instagram and Audience Network."[69]

111. Defendant also combines these customer lists with offline event data to effectively target PII Users. When advertisers create an ad campaign, Meta will "match the offline data [advertisers] upload to the event set so that [advertisers] can see how much [their] ads resulted in offline activity."[70] Meta also recommends that advertisers, like Defendant, provide an accurate timestamp for each event, down to "the minute or second."

---

[67] *Create a Customer Audience List*, FACEBOOK, HTTPS://WWW.FACEBOOK.COM/BUSINESS/HELP/170456843145568?ID=24690979533764 (last visited September 17, 2024).

[68] *Id.*

[69] *Customer List Custom Audiences*, FACEBOOK, HTTPS://WWW.FACEBOOK.COM/BUSINESS/HELP/341425252616329?ID=24690979533764 (last visited September 17, 2024).

[70] *Upload Offline Event Data*, FACEBOOK, HTTPS://WWW.FACEBOOK.COM/BUSINESS/HELP/155437961572700?ID=56590011044754 (last visited September 17, 2024).

.

112. Defendant uploaded customer lists and offline events so it can match a PII Users' video game searches, requests, purchases, and downloads with their corresponding Facebook profile.

VI. The Wiretap Statutes

a. California Invasion of Privacy Act

113. CIPA was enacted in 1967 for the expressly stated purpose "to protect the right of privacy of the people of [California]."[71] The California legislators were concerned about emergent technologies that allowed for the "eavesdropping upon private communications," believing such technologies "created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and civilized society."[72]

114. CIPA is regularly recognized as California's analog to the Federal Wiretap Act, comprised of the same general elements and protect against the same general harms.

115. To protect people's privacy, legislators broadly protected wired and aural communications being sent to or received from California.[73] Notably, for wired communications, California set out to prohibit (i) intentional wiretapping or (ii) willful attempts to learn the contents of wired communications, (iii) attempts to use or transmit information obtained through wiretapping, or (vi) aiding, agreeing with, employing, or conspiring with any person(s) to unlawfully do, permit, or cause the preceding three wrongs.[74]

116. CIPA claims are often treated as analogous to Wiretap Act claims.

b. The Federal Wiretap Act

117. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[75]

---

[71] Cal. Penal Code § 630
[72] *Id.*
[73] Cal. Penal Code § 631-32.
[74] *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1134 (E.D. Cal. 2021) (citing *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978)).
[75] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, WASH. & LEE J. C.R. & SOC. JUST.,

118. The Wiretap Act primarily concerned the government's use of wiretaps but was amended in 1986 through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[76]

119. Congress was concerned that technological advancements like "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing"[77] were rendering the Wiretap Act out-of-date, Congress amended the Wiretap Act in 1986 through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[78]

120. As a result, the ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third party processing of data and files.[79]

121. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

122. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

---

https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited September 17, 2024).

[76] *Id.* at 192.

[77] Senate Rep. No. 99-541, at 2 (1986).

[78] *Id.* at 192.

[79] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

123. While communicating with Defendant on the Website, users had the contents[80] of their communications with Defendant intercepted by Meta via the Pixel.

124. Defendant purposefully included the Pixel on the Website to intercept Plaintiffs' communications and redirect them to Meta to improve the effectiveness of its and Meta's advertising and marketing.

125. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant to Meta.

126. Defendant acted with the intent to have Plaintiffs' communications intercepted by Meta to use PII Users' protected, private information for their economic benefit through monetization the information via targeted advertising, and other means.

CLASS ACTION ALLEGATIONS

127. Plaintiffs bring this action individually and on behalf of the following Classes:

> All PII Users on the Website that had their PII, search terms, and detailed webpage information improperly intercepted by and disclosed to Facebook through the use of the Pixel (the "Class").
>
> All PII Users, who reside and used the Website in California, that had their PII, search terms, and detailed webpage information improperly intercepted by and disclosed to Facebook through the use of the Pixel (the "California Subclass").

128. Specifically excluded from the Class is Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

129. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

---

[80] The contents of Plaintiffs' and users' communications include: 1) search terms submitted to the site; 2) the location and contents of webpages visited by users; and, 3) the PII discussed in Section V.

130. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

131. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs did not know the exact number of members of the aforementioned Class. However, given the popularity of Defendant's Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

132. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, subscribed to, and used, the Website to access video games containing cut scenes, and had their PII collected and disclosed by Defendant.

133. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

134. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

135. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

1) Whether Defendant collected Plaintiffs' and the Class's PII and Video Watching Data;

2) Whether Defendant unlawfully disclosed and continues to disclose the PII and Video Watching Data of Subscribers of the Website in violation of the VPPA;

3) Whether Defendant' disclosures were committed knowingly; and

4) Whether Defendant disclosed Plaintiffs' and the Class's PII without consent.

136. Information concerning Defendant's Website data sharing practices and subscription members is available from Defendant's or third-party records.

137. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

138. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

139. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

140. Given that Defendant's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

///

///

///

CAUSES OF ACTION

COUNT I
VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, et seq.
(On behalf of Plaintiffs and the Class)

141. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 27 through 125 as though fully set forth herein.

142. Plaintiffs bring this count on behalf of himself and all members of the Class.

143. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d)." 18 U.S.C. § 2710(b)(1).

144. Defendant violated this statute by knowingly disclosing Plaintiffs' and other Class Members' personally identifiable information to Facebook.

145. Defendant, through the Website, engages in the business of delivering video content to subscribers, including Plaintiffs and the other Class Members, and other users. The Website delivers video games containing cut scenes to PII Users, including Plaintiffs and the other Class Members, by electronically sending those materials to Plaintiffs and the other Class Members on the Website who chose to download them.

146. "Personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

147. A "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

148. Defendant is a "video tape service provider" because it creates, hosts, and delivers hundreds of video games on its Website, thereby "engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio-visual materials." 18 U.S.C. § 2710(a)(4).

149. Defendant solicits individuals to purchase or subscribe to the Website to unlock access to video games published or produced by Defendant.

150. Plaintiffs and members of the Class are "consumers" because they paid money for individual games directly (Purchasers) or for a membership to Ubisoft+, which unlocked exclusive access to dozens of video games (Subscribers). 18 U.S.C. § 2710(a)(1).

151. Plaintiffs and the Class Members searched for, purchased, or download video games containing cut scenes using the Website.

152. Defendant disclosed Plaintiffs' and the Class Members' personally identifiable information to Facebook. Defendant utilized the Pixel which forced Plaintiffs' web browsers to transfer Plaintiffs' identifying information, like their Facebook IDs, along with Plaintiffs' event data, like the titles of the video games they searched for, purchased, or downloaded.

153. Defendant knowingly disclosed Plaintiffs' PII, which is triggered automatically through Defendant's use of the Pixel. No additional steps on the part of the Defendant, Facebook, or any third-party are required. And, once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID.

154. The VPPA provides that a videotape service provider may disclose personally identifiable information concerning a consumer as long as that person has provided "informed written consent . . . in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer." 18 U.S.C. § 2710(b)(2)(A)(i).

155. Plaintiffs and Class Members did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to third parties. Defendant failed to obtain "informed, written consent" from PII Users – including Plaintiffs and Class Members – "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and "at the election of the consumer," either "given at the time the disclosure is

sought" or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner." 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

156. Defendant's use of Plaintiffs' and Class Members' PII for marketing purposes was also prohibited. PII may be disclosed "for the exclusive use of marketing goods and services directly to the consumer" only where "the disclosure is solely of the names and addresses of consumers ***and*** . . . the disclosure does not identify the title, [or] description, . . . of any . . . audio visual material[.]" 18 U.S.C. § 2710(b)(2)(D); (b)(2)(D)(ii) (emphasis added). Here, Defendant did disclose Plaintiffs' and Class Members' PII, including video game titles, for solely marketing purposes.

157. Defendant's disclosure of Plaintiffs' and Class Members' PII was not made in the "ordinary course of business" as the term is defined by the VPPA. In particular, Defendant's disclosures to Facebook were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2).

158. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

159. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with VPPA's requirements for protecting a consumer's PII; (iii) statutory damages of $2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c) as to Defendant; and (iv) reasonable attorneys' fees and costs and other litigation expenses.

///

///

///

COUNT II
VIOLATION OF COMMON LAW INVASION OF PRIVACY
Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 27 through 125 as though fully set forth herein.

161. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

162. Plaintiffs and Class Members maintained a reasonable expectation of privacy in their communications with Defendant via its Website. Users' search terms, browsing history, geolocation data, and website activity have been recognized by society as sensitive information.[81]

163. Plaintiffs' and Class Members' reasonable expectation of privacy is supported by the VPPA's recognition that PII is sensitive information that must be protected from unauthorized disclosure.

164. Plaintiffs and Class Members maintained a reasonable expectation of privacy believing that Defendant would not share their search terms, browsing history, and PII with Defendant, as a VTSP, because Defendant was under a duty to not share such information with Meta unless Defendant had explicit authorization to do so.

165. Plaintiffs and members of the Class have an interest in: (i) precluding the dissemination and/or misuse of their sensitive and confidential information; and (ii) being free to search for and consume audio video materials without observation, intrusion or interference, including, but not limited to, the right to visit and interact with internet websites without being subjected to wiretaps without Plaintiffs' and Class Members' knowledge or consent.

166. Plaintiffs and Class Members possessed a reasonable expectation of privacy based on the belief that Defendant would abide by state criminal laws, such as CIPA. CIPA prohibits

[81] For example, California voted to pass the California Consumer Privacy Act of 2018, and voted to amend it in 2020 through Proposition 24, the California Privacy Rights Act (CPRA). The CPRA sets out that colling and using "personal information," including real names, online identifiers, internet browsing and search history, location data, audio and visual information, etc., requires businesses to provide adequate notice of such practices. *See generally* Cal. Civ. Code §§1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.140(v).

Facebook from intercepting communications between consumers, such as Plaintiffs and the Class, and their VTSPs without the consent of all parties involved in the communication. Through its placement of Pixel on the Website, Defendant enabled this interception and resulting intrusion upon Plaintiffs' and Nationwide Class Member's privacy.

167. As explained above, Healthcare Defendant's actions constitute a serious invasion of privacy that was egregious breach of social norms, such that the breach was highly offensive to a reasonable person because:

i. the invasion of privacy occurred in a highly sensitive setting – PII Users communications with the Defendant;

ii. Defendant had no legitimate objective or motive in invading Plaintiffs' and Class Members' privacy in such a manner;

iii. Defendant violated multiple laws by invading Plaintiffs' and Class Members' privacy, including CIPA and the Wiretap Act;

iv. Defendant deprived Plaintiff and Class Members of the ability to control dissemination of their search terms, browsing history, and PII; and

v. Defendant's actions are also unacceptable as a matter of public policy because they undermine the relationship between consumers and their video tape service providers.

168. Within the relevant time period, by implementing the Pixel on the Website, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights, and procured Meta to do so.

169. As a direct and proximate result of this infringement upon their privacy, Plaintiffs and Class Members sustained harm and experienced various damages. In light of this injury, Plaintiffs and Class Members are pursuing suitable remedies, such as compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court deems appropriate and fair.

COUNT III

Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of Plaintiff Lakes and the California Subclass)

170. Plaintiff Lakes incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 27 through 125 as though fully set forth herein.

171. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

172. California voters added the word "and privacy" to the California Constitution when they passed Proposition 11 in 1972. Proposition 11 is also known as the "Privacy Initiative" or "Right to Privacy Initiative."

173. In support to Proposition 11, voters stated that: The right of privacy is the right to be left alone … It prevents government and business and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

174. Plaintiff Lakes and the California Subclass Members have a legally protected interest in their PII and other information they send and receive to search for, request, purchase, or download video games containing cut scenes from Defendant through the Website, which Defendant violated by providing access to that data to Meta, which intercepted such communications. Plaintiff Lakes' and California Subclass Members' protected interests come from various statutes and common law, including:

a. VPPA;

b. The Wiretap Act;

c. CIPA;

d. The California Constitution, which protects the rights of privacy, and includes the "the ability to control circulation of our personal information;" and

e. Facebook's contracts, which "require each of these partners to have lawful rights to … share your data before providing any data to" Facebook.

175. The privacy rights of Plaintiff Lakes the California Subclass Members were invaded through the interception and collection of the data transmitted between PII Users' and their VTSP, here Defendant, which included their PII and other sensitive information, without first obtaining authorization or consent from Plaintiff Lakes and California Subclass Members.

176. Plaintiff Lakes and California Subclass Members had a reasonable expectation of privacy when communicating with Defendant online and thereby providing their PII to their VTSP. Plaintiff Lakes and California Subclass Members had a reasonable expectation of privacy when communicating with Defendant online and thereby providing their PII to their VTSP. It is widely recognized that video watching data cannot be shared with third parties without a consumer's consent.

177. This reasonable expectation of privacy in their PII harbored by Plaintiff Lakes and California Subclass Members is supported by VPPA's recognition that video watching information is sensitive information. This reasonable expectation of privacy in their PII harbored by Plaintiff Lakes and California Subclass Members is supported by VPPA's recognition that video watching information is sensitive information.

178. Plaintiff Lakes' and California Subclass Members' reasonable expectation of privacy is further supported by Facebook's affirmative promise that it would require its partners to only share data with Facebook that could be lawfully shared.

179. Plaintiff Lakes and California Subclass Members maintained a reasonable expectation of privacy in their PII supported further by their understanding that Facebook would not violate state criminal laws, such as the CIPA, in intercepting their communications with healthcare providers without the consent of both parties to the communications. Plaintiff Lakes and California Subclass Members maintained a reasonable expectation of privacy in their PII supported further by their understanding that Facebook would not violate state criminal laws, such as the CIPA, in intercepting their communications with healthcare providers without the consent of both parties to the communications.

180. As detailed above, Healthcare Defendant's acts in intercepting Plaintiff Lakes' and California Subclass Member's communications constitute a serious violation of social norms, and as such their breach is highly offensive to a reasonable person for the following reasons:

181. There was no legitimate objective for or motive for Defendant in invading Plaintiff Lakes' and California Subclass Member's privacy rights;

182. Defendant did not allow Plaintiff Lakes and California Subclass Members the ability to control the dissemination of their personal video game information;

183. Multiple laws, including the Wiretap Act and California Invasion of Privacy Act, were violated due to Facebook's invasion of Plaintiff Lakes' and California Subclass Members' privacy;

184. The context of the communication between Plaintiffs, California Subclass, and their healthcare providers is highly sensitive; and

185. Public policy also dictates that Defendant's actions undermine the relationship between Plaintiffs, the California Subclass, and VTSPs.

186. Plaintiff Lakes and California Subclass Members were injured and suffered damages as a direct and proximate result of Facebook's actions in invading their privacy rights. Thus, Plaintiff Lakes and California Subclass Members seek relief for those injuries including compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court may deem just and proper.

COUNT IV
VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § 2710, *et seq*.
(On Behalf of Plaintiffs and the Class)

187. Plaintiffs hereby incorporate by reference and re-allege herein the allegations contained in paragraphs 27 through 125 preceding paragraphs of this complaint.

188. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against the Defendant.

189. Codified under 18 U.S.C. U.S.C. §§ 2510 *et seq.*, the Federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

190. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

191. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

192. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

193. The Wiretap Act defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

194. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

195. The Defendant is a person for the purposes of the Wiretap Act.

196. The Pixel and other tracking tools constitute a "device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

197. The confidential communications Plaintiffs and members of the Class had with the Website, in the form of their search terms, browsing information, and PII, were intercepted by the tracking entities and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

198. Plaintiffs and members of the Class had a reasonable expectation of privacy in their electronic communications with the Website in the form of their Search Terms submitted to the Website and browsing information. Even if Plaintiffs and members of the Class would not

have had reasonable expectation of privacy in the electronic communications normally, Plaintiffs' and Class Members' electronic communications with the Websites included descriptions and summaries of the video games containing cut scenes they searched for, purchased, or subscribed to Ubisoft+ to unlock access to, along with their identifying information, giving rise to a reasonable expectation of privacy pursuant to the VPPA.

199. Plaintiffs and members of the Class reasonably expected that third parties were not intercepting, recording, or disclosing their electronic communications with the Website.

200. Within the relevant time period, the electronic communications between Plaintiffs and members of the Class and the Website were intercepted by the Pixel the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their private information, which includes the purpose of using such private information to develop advertising and marketing strategies.

201. Interception of Plaintiffs' and Class Members' confidential communications with the Website occur whenever a user uses the search bar within the Website, and when navigating various webpages of the Website.

202. At all times relevant to this Complaint, the Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Pixel and other tracking tools, including that allowing the tracking tools to be implemented on the Website would cause the private communications of their subscribers to be shared with third parties.

203. Plaintiffs and members of the Class were never asked for their consent to expose their confidential electronic communications with Website to third parties. Indeed, such consent could not have been given as Meta and Defendant never sought any form of consent from Plaintiffs or members of the Class to intercept, record, and disclose their private communications with the Website.

204. As detailed above, the tracking entities' unauthorized interception, disclosure and use of Plaintiffs' and the Class Members' confidential communications was only possible through

the Defendant's knowing, willful, or intentional placement of the tracking tools on the Website. 18 U.S. Code § 2511(1)(a).

205. Plaintiffs and members of the Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiffs and members of the Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and members of the Class and any profits made by the tracking entities as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) appropriate equitable or declaratory relief; (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT V
VIOLATION OF THE CALIFORNIA'S INVASION OF PRIVACY ACT
Cal. Penal Code § 631
(On Behalf of Plaintiff Lakes and California Subclass)

206. Plaintiff Lakes hereby incorporate by reference and re-alleges herein the allegations contained in paragraphs 27 through 125 of this complaint.

207. Plaintiff Lakes brings this count on behalf of himself and all members of the California Subclass.

208. CIPA provides that a person is liable to another where, "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following: (i) intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system; or (ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or (iii) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or (iv) aids, agrees

with, employs, or conspires with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section. Cal. Penal Code Section 631(a).

209. The Ninth Circuit has confirmed that one of the purposes of wiretapping statutes is to "prevent the acquisition of the contents of a message by an unauthorized third-party . . . ." *In re Facebook Internet Tracking Litig*., 956 F.3d 589, 608 (9th Cir. 2020). In dealing specifically with CIPA, the California Supreme court has similarly concluded that the objective of CIPA is to protect a person's communications "from a situation where the other person on the other end of the line permits an outsider" to monitor the communication. *Ribas v. Clark*, 38 Cal. 3d 355, 363 (1985); see *Smith v. LoanMe*, 11 Cal. 5th 183, 200 (2021).

210. The Website, including the Pixel placed upon it, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

211. Similarly, user's internet browsers, when instructed to transmit data by the Defendant's Pixel, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

212. Within the relevant time period, Plaintiff Lakes and members of the California Subclass:

a. used the search function to find video games on the Website;

b. navigated the Website to find webpages containing video games;

c. used the Website to subscribe to Ubisoft+;

d. used the Website to purchase and/or download video games.

213. Within the relevant time period, Meta, without the consent of all parties to the communication, or in any unauthorized manner, willfully read, or attempted to read, or learn the contents or meaning of electronic communications of Plaintiff Lakes and the putative California Subclass Members, contemporaneous with the communications transit through or passing over any wire, line or cable or with the communications sending from or being received at any place within California.

214. The information collected by Meta was not for the sole benefit of the Defendant.

215. Within the relevant time period, Defendant also aided, agreed with, conspired with, and employed tracking tools to accomplish the wrongful conduct at issue here.

216. Plaintiff Lakes and members of the California Subclass did not authorize or consent to the tracking, interception, and collection of any of their electronic communications.

217. The violation of section 631 constitutes an invasion of privacy sufficient to confer Article III standing.

Injunctive Relief of Defendant's Ongoing VPPA and Wiretap Violations

218. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative class they seek to represent, and Defendant, which parties have genuine and opposing interest in and which their interests are direct and substantial. Defendant has violated, and continue to violate, Plaintiffs' rights to protection of their PII under the VPPA.

219. Plaintiffs demonstrated that they are likely to succeed on the merits of their claims, and are thus, entitled to declaratory and injunctive relief.

220. Plaintiffs has no adequate remedy at law to stop the continuing violations of the VPPA by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the privacy rights of Plaintiffs and the absent Class Members and will continue to cause, or allow to be caused, irreparable harm to Plaintiffs. Injunctive relief is in the public interest to protect the PII of Plaintiffs, and other consumers that would be irreparably harmed through continued disclosure of their PII.

221. Defendant disregards its obligation under the VPPA by installing the tracking methods, including the Pixel, onto the Website and facilitating the sharing of subscribers' PII with third parties for any ordinary person to access and use.

222. Despite brazenly violating the VPPA, subscribers were provided with no notice of the employment of the Pixel and no indication of how or how much of their information was shared with third parties. Worse, in further violation of the VPPA, Defendant did not seek or obtain any form of consent from subscribers for the use of the tracking methods to share information improperly obtained from the Website.

223. This threat of injury to Plaintiffs from the continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure their PII is protected from future disclosure without adequate notice and consent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring that the Defendant's conduct violates the statute referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to, requiring Defendant to immediately (i) remove the Pixel from the Website or (ii) add, and obtain, the appropriate consent from subscribers;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) An award of statutory damages or penalties to the extent available;

(g) For Defendant to pay $2,500.00 to Plaintiffs and each Class Member, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);

(h) For pre-judgment interest on all amounts awarded;

(i) For an order of restitution and all other forms of monetary relief;

(j) An award of all reasonable attorneys' fees and costs; and

(k) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 3, 2024

PEIFFER WOLF CARR KANE CONWAY & WISE, LLP

By: /s/ *Sara B. Craig*
SARA BETH CRAIG (Bar No. 301290)
555 Montgomery Street, Ste. 820
San Francisco, CA 94111
Telephone: 415-766-3544
Facsimile: 415-840-9435
Email: scraig@peifferwolf.com

Brandon Wise*
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
One US Bank Plaza, Ste. 1950
St. Louis, MO 63101
Telephone: (314) 669-3600
Facsimile: (314) 898-9205
Email: bwise@peifferwolf.com

Mark S. Reich*
Colin A. Brown*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cbrown@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming